

# UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. **1:20-MJ-00560**

Information Associated with the Cellphone Assigned Call  
Number (772) 485-5027, with IMSI 310410785613395,  
that is Stored at Premises Controlled by AT&T Mobility

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

located in the Southern District of Florida, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1028(a)(7); 1028A; 1343; 1349	Unlawful transfer, possession, or use of a means of ID; aggravated ID theft; wire fraud; conspiracy to commit wire fraud

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days: ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I, an attorney for the government, certify that the information likely to be obtained is relevant to an ongoing investigation being conducted by TIGTA. See 18 U.S.C. §§ 3122(b), 3123(b).



Applicant's signature

Sean Williams, Special Agent, TIGTA

Printed name and title



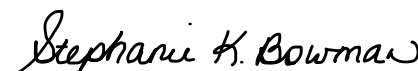
AUSA Julie D. Garcia

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

**FaceTime Video**

(specify reliable electronic means).

Date: Jul 22, 2020



Judge's signature

City and state: Cincinnati, Ohio

Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



**ATTACHMENT A**  
**Property to Be Searched**

1. The cellular telephone assigned call number **(772) 485-5027**, with International Mobile Subscriber Identity 310410785613395 / Electronic Serial Number 310410785613395, and listed subscriber(s) ADESH BISSOON (the “**TARGET CELL PHONE**”), whose service provider is AT&T Mobility (AT&T), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408.
2. All records and information associated with the **TARGET CELL PHONE** that are within the possession, custody, or control of AT&T, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

**ATTACHMENT B**  
**Particular Things to be Seized**

**I. Information to be Disclosed by the Provider**

1. All information about the location of the **TARGET CELL PHONE** described in Attachment A for a period of thirty days from the date of the warrant, during all times of day and night. “Information about the location of the **TARGET CELL PHONE**” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

2. To the extent that the information described in the previous paragraph (hereinafter, “Prospective Location Information”) is within the possession, custody, or control of AT&T MOBILITY, AT&T MOBILITY is required to disclose the Prospective Location Information to the government. In addition, AT&T MOBILITY must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Prospective Location Information unobtrusively and with a minimum of interference with AT&T MOBILITY’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on AT&T MOBILITY’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate AT&T MOBILITY for reasonable expenses incurred in furnishing such facilities or assistance.

3. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

## **II. Information to Be Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud) involving ADESH BISSOON, MICHAEL JOSEPH, VICTOR TORRES, or any co-conspirators.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the AT&T MOBILITY in order to locate the things particularly described in this warrant.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
THE CELLPHONE ASSIGNED CALL  
NUMBER (772) 485-5027, WITH IMSI  
310410785613395, THAT IS STORED AT  
PREMISES CONTROLLED BY AT&T  
MOBILITY

**Case No. 1:20-MJ-00560**

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Sean Williams being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **(772) 485-5027**, with International Mobile Subscriber Identity 310410785613395 / Electronic Serial Number 310410785613395, and listed subscriber ADESH BISSOON (the “**TARGET CELL PHONE**”), whose service provider is AT&T Mobility (“AT&T”), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408. The **TARGET CELL PHONE** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§

3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

3. I am a Special Agent with the United States Treasury Department, Treasury Inspector General for Tax Administration (“TIGTA”). TIGTA is tasked with ensuring the integrity of the Internal Revenue Service (“IRS”) and its infrastructure security and protecting the IRS against external attempts to corrupt tax administration. TIGTA special agents are certified criminal investigators with authority to carry firearms, make arrests, execute warrants, and administer oaths. I am assigned as a Criminal Investigator within the Cincinnati Field Office. I am also a member of TIGTA’s Cyber Investigative Cadre, whose mission is focused on communications- and computer network-related investigations. I have been employed by TIGTA since 2018. Prior to my employment with TIGTA, I was a special agent, investigator, and police officer with multiple U.S. federal government agencies. I have received training from the National Cyber-Forensics and Training Alliance and TIGTA’s Cybercrimes Investigative Division. Through my training and experience with these types of investigations, I have encountered a number of situations where email, the Internet, and other technologies have been employed to conduct criminal activity. As a Special Agent, I continue to receive training and education related to the investigation and prosecution of computer and other high-tech related crimes.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), among others, have been, are being, and will be committed by the user of the **TARGET CELL PHONE**. There is also probable cause to believe that the information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

6. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a “district court of the United States . . . that . . . has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **PROBABLE CAUSE**

**A. The government is investigating a suspected identity-theft scheme in which multiple subjects have exchanged stolen PII and fraudulent documents by email.**

7. The U.S. Attorney’s Office for the Southern District of Ohio and TIGTA are investigating a suspected identity-theft ring in which victims’ stolen personally identifiable information (PII) is being shared between multiple subjects via email.

8. In 2019, search warrants were executed on email accounts used by suspect VICTOR TORRES. I reviewed the returns associated with these search warrants and found that TORRES’s email accounts had exchanged emails containing lists of many individuals’ PII and/or fraudulent identity documents (such as fraudulent Social Security cards) with various email addresses, including ABissoon26@gmail.com and JerryLaster403@yahoo.com. Some of the emails containing what appeared to be stolen PII dated back to 2011.

9. Based on my training and experience, the lists of PII and the fraudulent identity documents exchanged between these email accounts are consistent with a conspiracy to commit identity theft. Parallel investigations by TIGTA have shown that these types of materials have been used to open bank accounts and credit cards, and to apply for loans without authorization.

10. Based on my knowledge of this investigation, I believe that the identity-theft conspiracy described in this affidavit involves at least three co-conspirators—TORRES, MICHAEL JOSEPH, and ADESH BISSOON—and that BISSOON is the user of the **TARGET CELL PHONE**.

**B. In January 2020, agents executed a search warrant at TORRES's residence and found evidence that the TARGET CELL PHONE is used by coconspirator ADESH BISSOON.**

11. In January 2020, a search warrant was executed at TORRES's residence in Apollo Beach, Florida. During the search, agents discovered fraudulent credit cards, checks, driver's licenses, and other fraudulent documentation. I believe based on this evidence that TORRES and his co-conspirators were still engaged in identity theft as of January 2020.

12. During the examination of VICTOR TORRES's telephone, agents found messages between VICTOR TORRES and the **TARGET CELL PHONE**, sent using the messaging service WhatsApp. Records from AT&T show that the International Mobile Subscriber Identity ("IMSI") for the **TARGET CELL PHONE** is 310410785613395 and that the Electronic Serial Number is 310410785613395.

13. I believe for several reasons that the user of the **TARGET CELL PHONE** is ADESH BISSOON and that BISSOON is a co-conspirator in this scheme. First, the **TARGET CELL PHONE** is subscribed to "ADESH BISSOON," and credit cards under



BISSOON's name have been used to pay the wireless bill. Second, the name associated with TORRES's contact for the **TARGET CELL PHONE** was "ADESH." Third, as noted above, TORRES's email accounts exchanged emails containing lists of PII with ABissooon26@gmail.com, and the email signature associated with the latter account lists the name "ADESH BISSOON." Finally, during my review of the contents of email addresses associated with this scheme, I found pictures of an individual who I believe matches the driver's license photograph of BISSOON.

14. The messages exchanged in October 2019 between the **TARGET CELL PHONE** and TORRES revealed screenshots of what I believe was an attempted mobile deposit for \$950.53 by BISSOON into a PNC bank account in the name of F.K. I believe that F.K. is a victim of TORRES's and BISSOON's identity-theft scheme, because I know from reviewing emails from FIUKid30@gmail.com that F.K.'s name was contained in multiple lists of PII sent to or received by TORRES.

15. Specifically, on October 27, 2019, the **TARGET CELL PHONE** sent a text to TORRES saying, "Send Jerry a specimen for install tomorrow." TORRES responded, "\$950 sound good [sic]." I know from my review of emails from TORRES's accounts that TORRES and his co-conspirators, when writing emails or texts, often use the terms "specimen" and "food" to refer to materials containing stolen PII, such as fraudulent Social Security cards. I believe based on my training and experience that they use these code words in an attempt to hide the criminal nature of their communications. I also know that, as described above, the email address JerryLaster403@yahoo.com has sent suspected stolen PII

to, and received suspected stolen PII from, accounts associated with TORRES.<sup>1</sup> I therefore believe that when BISSOON directed TORRES to “[s]end Jerry a specimen for install tomorrow,” he meant that TORRES should send the email address JerryLaster403@yahoo.com a falsified document for use in connection with their identity-theft scheme.

16. Two days later, on October 29, 2019, the **TARGET CELL PHONE** sent a text to TORRES that said: “The thing got delayed until the 4th.” I believe BISSOON meant that the check would not be deposited until November 4th, because the next day, the **TARGET CELL PHONE** sent a text of a screenshot from the PNC bank account showing that a hold had been placed on a \$950.53 mobile deposit until November 4, 2019.

17. On October 31, 2019, the **TARGET CELL PHONE** texted TORRES a screenshot from the PNC bank account showing that a check deposited for \$950.53 had been returned unpaid because the bank believed it was altered and/or fictitious. Based on my training and experience, I believe this is additional evidence that the user of the **TARGET CELL PHONE**, who I believe is BISSOON, was attempting to deposit a fraudulent check in connection with the identity-theft scheme.

18. As of January 2020, when the search warrant at TORRES’s residence was executed and TORRES’s phone was seized, the last communication via text between TORRES and the **TARGET CELL PHONE** was on January 7, 2020. TORRES wrote, “Sent

---

<sup>1</sup> For example, in July 2019, the email address JerryLaster403@yahoo.com sent FIUKid30@gmail.com an email about a “schedule to create paper for players” that listed F.K.’s name. Based on my training and experience and knowledge of this investigation, including the nature of the emails exchanged between TORRES, BISSOON, and other individuals who I believe are their co-conspirators, I believe that when the user of JerryLaster403@yahoo.com referred to “creat[ing] paper for players,” he meant creating falsified paperwork using the listed individuals’ PII.

the paper to my friend Jason. He at the office working hard. Lol.” The **TARGET CELL PHONE** responded, “I will contact you soon with the requested information.” Based on my training and experience and knowledge of this investigation, I believe that, when TORRES referred to “the paper,” he meant falsified documents created using stolen PII, because I have seen several communications in which, based on context, I believe TORRES and his co-conspirators were using the term “paper” in that way.

19. Records from AT&T show that the **TARGET CELL PHONE** was activated under BISSOON’s name in 2005 and that, as of late May 2020, the device was still registered to BISSOON. For that reason, I believe there is probable cause that BISSOON is still using the **TARGET CELL PHONE**.

20. I am now seeking a search warrant for location information associated with the **TARGET CELL PHONE** to assist agents in surveilling the user of the **TARGET CELL PHONE** for the purpose of obtaining additional evidence of the scheme under investigation, including definitively identifying the user of the **TARGET CELL PHONE**.

#### **BACKGROUND ON AT&T AND LOCATION INFORMATION**

21. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data, and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal

using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (*i.e.*, face of the tower) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.

Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or GPS data.

22. Based on my training and experience, I know that AT&T can collect E-911 Phase II data about the location of the **TARGET CELL PHONE**, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on AT&T's network or with such other reference points as may be reasonably available.

23. Based on my training and experience, I know that AT&T can collect cell-site data about the **TARGET CELL PHONE**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as AT&T typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

**AUTHORIZATION REQUEST**

24. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

25. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **TARGET CELL PHONE** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

26. I further request that the Court direct AT&T to disclose to the government any information described in Attachment B that is within the possession, custody, or control of AT&T. I also request that the Court direct AT&T to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with AT&T's services, including by initiating a signal to determine the location of the **TARGET CELL**

**PHONE** on AT&T's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate AT&T for reasonable expenses incurred in furnishing such facilities or assistance.

27. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **TARGET CELL PHONE** outside of daytime hours.

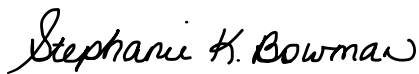
Respectfully submitted,



---

Sean Williams  
Special Agent  
Treasury Inspector General for Tax  
Administration (TIGTA)

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1 this 22 day of July, 2020, **via Facetime Video.**



---

THE HONORABLE STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**  
**Property to Be Searched**

1. The cellular telephone assigned call number **(772) 485-5027**, with International Mobile Subscriber Identity 310410785613395 / Electronic Serial Number 310410785613395, and listed subscriber(s) ADESH BISSOON (the “**TARGET CELL PHONE**”), whose service provider is AT&T Mobility (AT&T), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408.
2. All records and information associated with the **TARGET CELL PHONE** that are within the possession, custody, or control of AT&T, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

**ATTACHMENT B**  
**Particular Things to be Seized**

**I. Information to be Disclosed by the Provider**

1. All information about the location of the **TARGET CELL PHONE** described in Attachment A for a period of thirty days from the date of the warrant, during all times of day and night. “Information about the location of the **TARGET CELL PHONE**” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

2. To the extent that the information described in the previous paragraph (hereinafter, “Prospective Location Information”) is within the possession, custody, or control of AT&T MOBILITY, AT&T MOBILITY is required to disclose the Prospective Location Information to the government. In addition, AT&T MOBILITY must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Prospective Location Information unobtrusively and with a minimum of interference with AT&T MOBILITY’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on AT&T MOBILITY’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate AT&T MOBILITY for reasonable expenses incurred in furnishing such facilities or assistance.

3. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).



## **II. Information to Be Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud) involving ADESH BISSOON, MICHAEL JOSEPH, VICTOR TORRES, or any co-conspirators.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the AT&T MOBILITY in order to locate the things particularly described in this warrant.